AMENDMENT TO THE CLAIMS: This listing of claims replaces all prior versions.

1-23 (Cancelled)

24. (Currently amended) A method for effectively and efficiently identifying violations of privacy and security and guidelines in an information system while documentating and accommodating the live process of compliance and security testing, comprising the steps of:

a. providing vulnerability data having universal definitions applicable to different computing systems;
b. providing regulation data relating to and taken from a particular set of regulations;
c. providing priority data relating to a list of vulnerabilities prioritized in a specific order;
d. providing keywords that are common to the vulnerability, regulation and priority data;
e. searching for the keywords in the vulnerability, regulation and priority data.
f. creating relational data based upon the searching step, the relational data establishes a specific relationship between the vulnerability, regulation and priority data.
g. determining a computer configuration for a target to be tested;
h. customizing a screening process for the target using the computer configuration found in the determining step;
i. testing for vulnerability violations in the target based upon the customized screening process;

j. determining, according to the vulnerability violations, which regulation data applies to which vulnerability data and the priority of the vulnerability violations by a relational database for providing a mapping between the vulnerabilities and the regulations; and

k. creating a prioritized report corresponding to the vulnerability violations and the regulations that apply to the vulnerability violations.

25. (Previously Presented) The method of claim 24 wherein the set of regulations are defined by Health Insurance Portability and Accountability Act.

26. (Previously Presented) The method of claim 24 wherein the regulations are defined by Graham Leach Bailey Act.

27. (Previously Presented) The method of claim 24 wherein the vulnerability violations are stored in a memory.

28. (Previously Presented) The method of claim 24 wherein the testing step further comprises scanning a target to provide a system scan.

29. (Previously Presented) The method of claim 28 further comprising the step of providing a test set as a function of the system scan.

30. (Currently Amended) The method of claim 24 wherein the prioritized report further includes an IP address of the target.

31. (Previously Presented) The method of claim 24 wherein the vulnerabilities data is defined by Common Vulnerabilities and Exposures.

32. (Currently Amended) A information system for effectively and efficiently identifying violations of privacy and security and guidelines while documenting and accommodating the live process of compliance and security testing, comprising:

a. a vulnerability database having universal definitions applicable to different computing systems;

b. a regulation database taken from and relating to a particular set of regulations;

c. a priority database relating to a list of vulnerabilities prioritized in a specific order;

d. means for providing keywords that are common to the vulnerability, regulation and priority data;

e. searching means for keywords in the vulnerability, regulation and priority data;

f. a memory for storing relational data that was created by the searching means, the relational data establishes a specific relationship between the vulnerability, regulation and priority databases;

g. first determining means for determining a computer configuration for a target to be tested;

h. customizing means for customizing a screening process for the target using the computer configuration found in the first determining means;

i. testing means for testing for vulnerability violations in the target based upon the customized screening process;

j. second determining means for determining, according to the vulnerability violations, which regulation data applies to which vulnerability data and the priority of the vulnerability violations by a relational database for providing a mapping between the vulnerabilities and the regulations; and

k. a prioritized report corresponding to the vulnerability violations and the regulations that apply to the vulnerability violations.

33. (Previously Presented) The method of claim 32 wherein the set of regulations are defined by Health Insurance Portability and Accountability Act.

34. (Previously Presented) The method of claim 32 wherein the set of regulations are defined by Graham Leach Bailey Act.

35. (Previously Presented) The method of claim 32 wherein vulnerability violations are

stored in a memory.

36. (Previously Presented) The system of claim 32 wherein the testing means further comprises scanning a target to provide a system scan.

37. (Previously Presented) The system of claim 36 further comprising a test set as a function of the system scan.

38. (Previously Presented) The system of claim 32 wherein the prioritized report further includes an IP address of the target.

39. (Previously Presented) The system of claim 24 wherein the vulnerabilities data is defined by Common Vulnerabilities and Exposures.

40. (Currently amended) Computer-executable process steps, stored on a computer-readable medium and executable by a processor to perform the steps of:

a. document and accommodate a live process of compliance and security testing;

b. provide vulnerability data having universal definitions applicable to different computing systems;

c. provide regulation data taken from and relating to a particular set of regulations;

d. provide priority data relating to a list of vulnerabilities prioritized in a specific order;

e. provide keywords that are common to the vulnerability, regulation and priority data;

f. search for the keywords in the vulnerability, regulation and priority data;

g. create relational data based upon the search step, the relational data establishes a specific relationship between the vulnerability, regulation and priority databases;

h. determine a computer configuration for a target to be tested;

i. customize a screening process for the target using the computer configuration found in the determine step;

j. test for vulnerability violations in the target based upon the customized screening process;

k. determine, according to the vulnerability violations, which regulation data applies to which vulnerability data and the priority of the vulnerability violations by a relational database for providing a mapping between the vulnerabilities and the regulations ; and

l. create a prioritized report corresponding to the vulnerability violations and the regulations that apply to the vulnerability violations.

41. (Previously Presented) The steps of claim 10 wherein the set of regulations are defined by Health Insurance Portability and Accountability Act.

42. (Previously Presented) The steps of claim 40 wherein the set of regulations are defined by Graham Leach Bailey Act.

43. (Previously Presented) The steps of claim 40 wherein the test step further comprises scanning a target to provide a system scan.

44. (Previously Presented) The steps of claim 43 further comprising the step of providing a test set as a function of the system scan.

45. (Previously Presented) The steps of claim 40 wherein the prioritized report further includes an IP address of the target.

46. (Previously Presented) The steps of claim 40 wherein the vulnerabilities data is defined by Common Vulnerabilities and Exposures.